ETH Relay: A Cost-efficient Relay for Ethereum-based Blockchains

Philipp Frauenthaler, Marten Sigwart, Christof Spanring, Michael Sober, Stefan Schulte

Stefan Schulte
s.schulte@ds.g.tuwien.ac.at
Distributed Systems Group
TU Wien
Motivation: Blockchain Relays

- Promising way to break isolation between blockchains
- Relay is a smart contract acting as light node (relay contract)
- The relay contract can verify whether some transaction is included in another blockchain
- Fully decentralized
Motivation: Blockchain Relays – Limitations

- Validation of each received block header according to the protocol rules, e.g., consensus algorithm
- Ethereum-based blockchains use Ethash as consensus algorithm
- Validating Ethash on Ethereum-based blockchains expensive
  - around 3 million gas per header
- Ethereum: New block header every 14 seconds
- Validating each header leads to exorbitant operating cost

➢ Research Question 1: “How can we make relays economically more viable for Ethereum-based blockchains?”
Solution: Validation-on-demand

- Relay contract optimistically accepts new block headers
  - No validation of Ethash
- Since this may lead to invalid block headers entering the relay contract: New block headers locked for some time (lock period)
- Off-chain clients can dispute locked block headers
  - Triggers header validation incl. Ethash
  - If header indeed invalid \(\rightarrow\) Invalid block is removed from the relay contract
- After the lock period, headers are considered valid
Solution: Content-addressable Storage Pattern

- Further decrease storage consumption of the relay contract
- Store only some meta data of the block header in the relay contract
  - E.g., block hash, block number
- The full header is recorded in the transaction invoking the contract at submission
- Less storage consumption within the relay contract
- But: For each dispute and Simplified Payment Verification (SPV) execution full block must be provided
Solution: Incentive Structure

Research Question 2: “How can we motivate off-chain clients to participate and to behave honestly?”

• Compensate off-chain clients for submitting and disputing headers
  • For submitting headers
    • Every time the header is used for SPVs, the submitters of that header gets a fee
  • For disputing headers
    • For each header submission clients have to provide some stake (e.g., 1 ETH)
    • Stake is locked during the lock period of the header
    • If header is indeed invalid, disputer gets locked stake as reward
Evaluation: Settings

• Goal: Estimate the operational cost of ETH Relay
• Data set:
  • Collected 154,445 block headers containing 2,542 branches from the Ethereum main network (17.12.2019 to 14.01.2020)
• Three prototypical implementations

<table>
<thead>
<tr>
<th>Functionality</th>
<th>Baseline</th>
<th>ETH Relay 1</th>
<th>ETH Relay 2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Validation-on-submission</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Validation-on-demand</td>
<td></td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Content-addressable storage</td>
<td></td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>Naïve search</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Optimized search</td>
<td></td>
<td>✓</td>
<td>✓</td>
</tr>
</tbody>
</table>
Evaluation: Average Operating Cost per Header Submission

- Experiment No. 1: Operating cost, i.e., cost of submitting block headers and cost of on-chain SPVs
- Results: ETH Relay 1 is 82% cheaper than the baseline; ETH Relay 2 is 92% cheaper than the baseline
Evaluation: Average Operating Cost of On-chain SPVs

- Continuation of Experiment 1: After each header submission, an SPV on the Genesis block is triggered.
- Results: Cost grow with the number of submitted headers. Baseline is above 6.7 million gas after already 18,766 submitted headers.
Conclusion

- Research Question 1: “How can we make relays economically more viable for Ethereum-based blockchains?”
- Research Question 2: “How can we motivate off-chain clients to participate and to behave honestly?”
- Reduction of operating cost by up to 92 %

https://github.com/pantos-io/ethrelay
Thanks a lot for your attention!

Dr.-Ing. Stefan Schulte
Associate Professor

TU Wien Informatics
Research Unit Distributed Systems
Argentinierstraße 8/194-02 | 1040 Vienna | Austria
+43-1-58801-18417 | s.schulte@dsg.tuwien.ac.at
informatics.tuwien.ac.at | dsg.tuwien.ac.at/staff/sschulte
Evaluation: Cost of Header Disputes

- **Experiment 2**: Repeats Experiment 1, but now, we dispute the Genesis block (with a growing number of headers to be removed with each dispute)

- **Results**:
  - Temporary decline of cost, due to gas refund
  - ETH Relay 1 reaches gas limit much earlier than ETH Relay 2